What is Malvertising (Malicious Ads)?

Malvertising causes a lot of damage. In June 2015, Invincea estimated that the level of damage could reach billions of dollars and there was reason to believe that the malvertising rate would increase in the coming years.

Although it is difficult to determine the prevalence of malvertising, it is clearly a growing threat. Invincea, a security firm, blocked 2.1 million malicious ads in the first 6 months of 2015. RiskIQ has stated that the number of malicious ads counted during that period increased by 260% over the previous year. A huge number.

Malvertising causes a lot of damage. In June 2015, Invincea estimated that the level of damage could reach billions of dollars by the end of 2015. There is reason to believe that the malvertising rate will increase in the coming years.

This tutorial will help you understand what malvertising is, why it is becoming so popular, where it lurks and what you can do with it.

What is Malvertising (Malicious Ads)?

What is Malvertising?

"Malvertising" is a name for "malicious advertising". Basically, malvertising uses online advertising to infect different types of malware to computers.

The truth is, the computer may be infected with malware even if you don't click on the ad. Viewing ads only can cause malware to infect computers. There are no signs you can notice.

This is done by inserting a special script in the ad, as soon as it is displayed to the user; This is called 'pre-click' infection. Users can also get 'after clicking' and ads redirect users to bad websites, download malicious files to the computer. This is still an effective way to infect malware.

What will Malvertising bring to your computer? It can be anything from adware to a code that changes the settings on the router in your home. Exploiting toolkits often appear in malware. They will 'open' the computer

for any other type of malware that a cybercriminal wants to install on your hard drive, such as ransomware, botnet, and bank / financial information theft programs.

Why is malvertising becoming more popular?

The reason the incidents with malvertising are increasing is easy to explain: It really works very well.

One of the reasons it works so well is that it can effectively penetrate trusted sites. Third-party ad networks sell ads for major websites like eBay, Weather Channel, Rotten Tomatoes, etc., and those sites display ads. If a malicious ad finds a way to be accepted, it can be distributed to a large number of websites before being discovered.

Many transactions between advertisers and advertising networks are done by program, and people can only influence external factors, thereby increasing the chance for an advertiser to infect malicious advertising, through the advertising network's own security system. Sites that do not even know which ads will be displayed on their site (except for ad networks, who are responsible for the privacy of the ad).

Even highly reliable ad networks, such as Google's DoubleClick, have also distributed malicious ads. One method that malicious people use to get their ads on these trusted networks is by buying space for 'harmless' ads first; when they have established a reputation as a legitimate advertiser, they will start adding ads with malware. Because then they are less supervised than new advertisers. They take advantage of this vulnerability to spread malware before being detected.

A newer way to distribute malvertising is to assemble malware in time. This method includes seemingly harmless components in advertisements. They are downloaded separately to the victim's computer, before being assembled and compiled into complete malware. It can then run or download additional components to complete the assembly. This is especially difficult to detect.

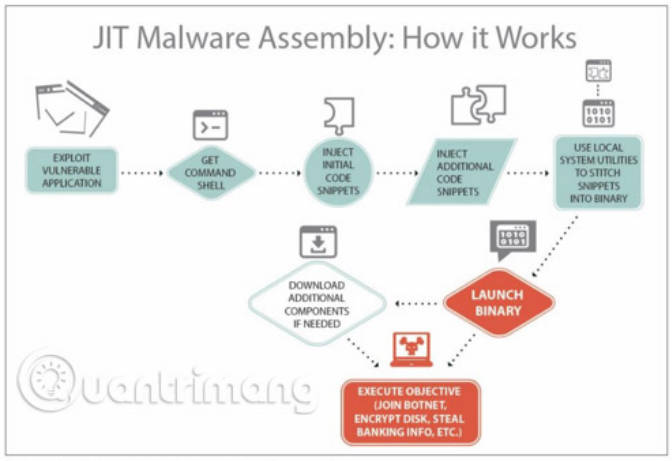


Figure 5: How JIT malware assembly works

Adware can also be installed via a browser add-on and malicious extension that many users are not wary of. This adware can trigger additional infection processes, through the use of distributions directly to the user's browser.

Where is Malvertising hiding?

Unfortunately, you can find malvertising anywhere. Of course, online and torrent sites are dangerous, but because third-party ad networks are active, ads infected with malware can spread to many other trusted sites with speed. fast.

And because many malware can spread without users clicking on ads, malvertising is extremely dangerous. However, RiskIQ's research shows that by 2015, the most common malicious form is through fake software updates, especially for Adobe's Flash plugin. They can also be spread through fake warnings about malware and viruses, although the ratio of this method has decreased. The warning below looks legitimate, but be careful before clicking the link to make sure you know how to detect a fake link.

This is why it is difficult to protect yourself from malicious software: They attack very quickly and can come from anywhere.

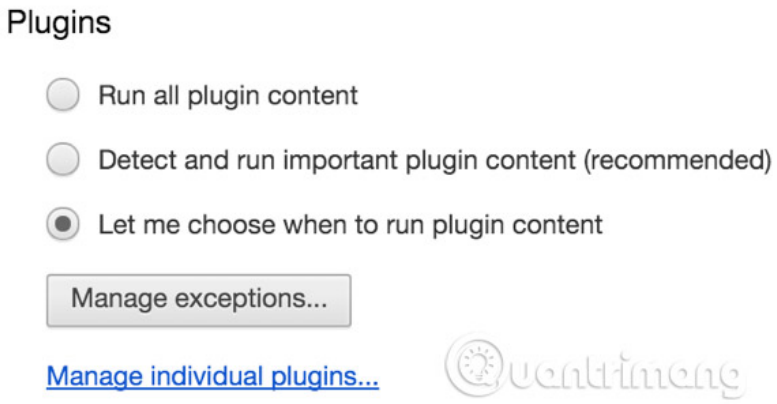
How to protect yourself from malvertising

The steps to protect yourself from being attacked by malicious ads are very similar to the steps you need to take to protect yourself from any other type of malware.

Turn off Flash and Silverlight

1. Instructions to disable Flash Player on all browsers

Adobe's Flash and Silverlight are often targeted by cyber criminals to exploit, due to their common security vulnerabilities. If you are running one of these plugins in your browser, you should turn them off immediately or at least enable the click-to-play feature so that you are prompted to approve the plugin usage, before it starts.



And then, of course, you should only approve the use of Flash or Silverlight, if you are confident that the site you are visiting is clean and the plugin is not required to advertise (for example, if you are using Amazon. Prime on Safari, you'll need to use Silverlight to stream videos online. However, Flash and Silverlight are not the only insecure plugins, so be sure to thoroughly understand which plugins you should turn off or restrict.

Block ads and scripts

It is a controversial fact, but now, it is the best way to protect yourself from being infected with malware. If the ad is blocked, the ad cannot infect you with malware. Blocking scripts will also help, as they are often tools embedded in fixes to spread malware.

Unfortunately, even trusted domains may not be absolutely safe due to the third-party revolution operating. There have been reports of malvertising contamination in LA Times, Yahoo, Comcast, Answers.com, and many other well-known websites. You never know where it will appear next.

Use antivirus software

At this point, if you do not use antivirus software, you are very likely to be infected with malware. There are many great antivirus options and they all work to protect you from malware.

Install antivirus software, make sure it always runs and updates the software regularly.

Malvertising is not a new issue, but its popularity is growing rapidly, so we may see more consequences in the coming years. And no matter how you feel about blocking ads, it is still the best way to stay safe. However, with the sophistication of cybercrime, that may not work long term.

Are you worried about malvertising? Have you started using ad blockers or scripts? Do you have any experience with malvertising? Share your thoughts in the comment section below!

See more:

1. Risks from malware and how to prevent it
2. 9 things to do when detecting a computer infected with malware
3. Completely remove Adware and Spyware on your system
4. How to identify computers infected with viruses with 10 characteristic signs